DECREE
No 82/2018 Coll.

of May 21, 2018

on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree)

The National Cyber and Information Security Agency, pursuant to Section 28, paragraph 2, letters a) to d) and f) of Act No. 181/2014 Coll., on Cybersecurity and on the Amendment to Related Acts (the Cybersecurity Act), as amended by Act No. 104/2017 Coll. and Act No. 205/2017 Coll. (hereinafter referred to as the "Act"), establishes as follows:

PART ONE

INTRODUCTORY PROVISIONS

Section 1

Scope

This Decree incorporates the relevant European Union law[1]) and for a critical information infrastructure information system, a critical information infrastructure communication system, an important information system, an essential service information system, or for an information system or an electronic communications network used by a digital service provider (hereinafter referred to as the "information and communication system") it establishes

a) the content and structure of security documentation,
b) the content and scope of security measures,
c) the types, categories and significance assessments of cybersecurity incidents,
d) the requirements and method for reporting a cybersecurity incident,
e) the details of notification of the implementation of a reactive measure and its outcome,
f) a sample notification of contact details and its form; and
g) the method of the disposal of data, operational data, information and copies thereof.

Section 2

Definition of terms

For the purposes of this Decree, the terms below are understood to have the following meanings:

a) "System administrator" is a person responsible for the management, operation, use, maintenance and safety of a technical asset,

[1]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures on a high common level of security of network and information systems across the Union.

b) “Acceptable risk” is risk acceptable to the authority or natural or legal person required to implement a security measure under the law (hereinafter referred to as the “obliged entity”) and it is not necessary to manage it through other security measures,
c) “Security policy” is a set of principles and rules that determine the method for asset protection,
d) “Risk assessment” is an overall process of risk identification, analysis and evaluation,
e) “Threat” is a potential cause of a cybersecurity event or a cyber security incident that may cause damage,
f) “Supporting asset” is a technical asset, the employees and suppliers involved in the operation, development, management or security of the information and communication system,
g) “Primary asset” is the information or service being processed or provided by the information and communication system,
h) “Risk” is the possibility that a particular threat will exploit the asset's vulnerability and cause damage,
i) “Risk management” is an activity involving a risk assessment, selection and implementation of risk management measures, the sharing of information related to risk, and risk monitoring and review,
j) “Information security management system” is a part of the obliged entity's management system based on access to the information and communication system risks, which provides for the establishment, implementation, operation, monitoring, review, maintenance and improvement of information and data security,
k) “Technical asset” is such technical equipment, means of communication and software of the information and communication system and the premises, in which these systems are located, the failure of which may have an impact on the information and communication system,
l) “User” is a natural or legal person or a public authority using the assets,
m) “Top management” is a person or a group of persons who are in charge of the obliged entity or a statutory body of the obliged entity,
n) “Important supplier” is an information or communication system administrator (hereinafter referred to as the "Administrator”) and anyone who enters with the obliged entity into a legal relationship, that is important to the security of the information and communication system,
o) “Important change” is a change that has or may have an impact on cybersecurity and poses a high risk,
p) “Vulnerability” is a weakness of an asset or a weakness of a security measure that can be exploited by one or more threats.

PART TWO

SECURITY MEASURES

TITLE I

ORGANISATIONAL MEASURES

Section 3

Information security management system

Within the framework of the information security management system, the obliged entity

a) defines, with regard to the requirements of the parties concernedand organisational security, the scope of the information Security Management System, specifying the organisational parts and assets covered by the information security management system,
b) establishes the objectives of the information security management system,
c) introduces adequate security measures for the defined scope of the information security management system based on the objectives of the information security management system, security needs, and risk assessment,
d) manages the risks pursuant to Section 5,
e) establishes and approves a security policy in the area of the information security management system, which includes guiding principles, objectives, security needs, rights and obligations in relation to the Information Security Management, and based on security needs and risk assessment outcomes establishes a security policy in other areas pursuant to Section 30 and introduces adequate security measures,
f) ensures that a cybersecurity audit of the Information and Communication System (hereinafter referred to as the "Cybersecurity Audit") is carried out pursuant to Section 16,
g) ensures that a regular evaluation of the effectiveness of the information security management system is carried out, which contains the assessment of the state of the information security management system, including a review of the risk assessment, an evaluation of results of cybersecurity audits carried out and the impacts of cybersecurity incidents on the information security management system,
h) continuously identifies and subsequently, pursuant to Section 11, manages important changes that fall within the scope of the information security management system,
i) keeps the information security management system and relevant documentation up to date on the basis of the findings of cybersecurity audits, the results of evaluation of the effectiveness of the information security management system and in connection with important changes made, and
j) manages the operations and resources of the information security management system and records any activities connected with the information security management system and risk management.

Section 4

Asset management

(1) Within the framework of asset management, the obliged entity

a) establishes a methodology for identifying assets,
b) establishes a methodology for assessing assets at least within the scope set out in Annex 1 hereto,
c) identifies and keeps records of assets,
d) determines and keeps records of asset guarantors,
e) assesses and keeps records of primary assets in terms of confidentiality, integrity and availability and classifies them to individual levels referred to in letter b),
f) identifies and keeps records of relations between the primary and the supporting assets and assesses the consequences of dependencies between the primary and the supporting assets,
g) assesses the supporting assets, taking into account in particular the interdependencies referred to in letter f),
h) establishes and implements, on the basis of asset assessments, the protection rules necessary to safeguard the individual levels of assets,
i) establishes the permissible ways of using assets and the asset handling rules with regard to the level of assets, including rules for secure electronic sharing and physical transfer of assets, and
j) determines the method of the disposal of data, traffic data, information and copies thereof or the disposal of technical data carriers with regard to the level of assets in accordance with Annex 4 hereto.

(2) When assessing the importance of primary assets, at least the following must be assessed

a) the extent and importance of personal data, special categories of personal data or business secrets,
b) the extent of legal obligations or other obligations in question,
c) the extent of disruption of internal management and control activities,
d) the damage to public, commercial or economic interests and possible financial losses,
e) impacts on the provision of important services,
f) the extent of disruption of routine activities,
g) impacts on the maintenance of good name or protection of reputation,
h) impacts on the health and safety of people,
i) impacts on international relations, and
j) impacts on users of the information and communication system.

Section 5

Risk management

(1) Within the framework of risk management in connection with Section 4, the obliged entity

a) establishes a methodology for risk assessment, including the establishment of risk acceptance criteria,
b) identifies relevant threats and vulnerabilities with respect to assets, while considering in particular the threats and vulnerabilities listed in Annex 3 hereto,
c) carries out risk assessments at regular intervals pursuant to paragraph 2 and in case of important changes,
d) takes into account relevant threats and vulnerabilities in the risk assessment and evaluates possible impacts on assets; these risks are assessed at least within the scope of Annex 2 hereto,
e) prepares a risk assessment report,
f) prepares, on the basis of security needs and the results of the risk assessment, a declaration of applicability, which contains an overview of security measures required by this Decree, which
    1. were not applied, including justification,
    2. were applied, including the manner of fulfilment,
g) develops and implements a risk management plan that includes the objectives and benefits of security measures for managing individual risks, identifying a person to enforce security risk management measures, the necessary financial, technical, human and information resources, the deadline for their implementation, description of the relations between the risks and appropriate security measures and the way to implement the security measures,
h) takes into account, within the risk assessment and in the risk management plan,
    1. important changes,
    2. changes in the scope of the information security management system,
    3. measures pursuant to Section 11 of the Act, and
    4. cybersecurity incidents, including those previously addressed, and
i) introduces security measures in line with the risk management plan.

(2) The obliged entity referred to in Section 3, letters c), d) and f) of the Act carries out the risk assessment at least once a year and the obliged entity referred to in Section 3, letter e) of the Act at least every three years.

(3) Risk management may be provided in ways other than those set out in paragraph 1 letter d) if the obliged entity ensures that the measures applied provide the same or higher level of the risk management process.

Section 6

Organisational security

(1) With regard to the information security management system, the obliged entity

a) ensures the establishment of the security policy and objectives of the information security management system referred to in Section 3, consistent with the strategic direction of the obliged entity,

b) ensures the integration of the information security management system into the obliged entity's processes,
c) ensures the availability of the resources needed for the information security management system,
d) informs employees of the importance of the information security management system and of the importance of achieving compliance with its requirements with all parties concerned,
e) provides support to achieve the intended outputs of the information security management system,
f) guides employees to develop the effectiveness of the information security management system and encourages them in this development,
g) advances the continuous improvement of the information security management system,
h) supports persons playing security roles in advancing cybersecurity in their areas of responsibility,
i) ensures that rules are set for the designation of system administrators and security role holders,
j) ensures that the confidentiality of system administrators and security role holders is maintained,
k) ensures appropriate powers and resources for security role holders, including budgetary means, in fulfilling their roles and performing related tasks, and
l) ensures the testing of continuity plans for activities, recovery, and cybersecurity incident management processes.

(2) The obliged entity within the information security management system determines the composition of the Cybersecurity Management Committee and their security roles and their rights and obligations related to the information security management system.

(3) The obliged entity referred to in Section 3, letters c), d) and f) of the Act designates a person who will hold the security role of

a) a cybersecurity manager,
b) a cybersecurity architect,
c) an asset guarantor, and
d) a cybersecurity auditor.

(4) The obliged entity referred to in Section 3, letter e) of the Act determines the roles of the cybersecurity manager and asset guarantor. Other security roles pursuant to paragraph 3 are to be determined proportionately to the scope and requirements of the information security management system.

(5) The obliged entity referred to in Section 3, letters c), d) and f) of the Act ensures the substitutability of the security roles referred to in paragraph 3, letters a) and b).

(6) The obliged entity referred to in Section 3, letter e) of the Act ensures the substitutability of the security role of a cybersecurity manager.

(7) The Cybersecurity Management Committee is composed of persons with appropriate competences and expertise for the overall management and development of the information security management system and persons significantly involved in the management and coordination of cybersecurity activities; between its members there must be at least one top management representative or a person authorized by it and a cybersecurity manager. For the Cybersecurity Management Committee, the obliged entity takes into account the recommendations referred to in Annex 6 hereto.

Section 7

Security roles

(1) The cybersecurity manager

a) is a security role responsible for the information security management system; the exercise of this role may be entrusted to a person trained for this activity and demonstrating professional competence in cybersecurity management or information security management
   1. for a period of at least three years, or
   2. for a period of one year when graduated from university;

b) is responsible for informing the top management on a regular basis on
   1. activities resulting from the scope of his or her responsibility, and
   2. on the state of the information security management system, and

c) must not be entrusted with exercising the roles responsible for operation of the information and communication system.

(2) The cybersecurity architect is a security role responsible for drafting the implementation of security measures to ensure a secure architecture of the information and communication system; the exercise of this role may be entrusted to a person trained for this activity and demonstrating professional competence in designing implementation of security measures and security architecture

   a) for a period of at least three years, or
   b) for a period of one year when graduated from university.

(3) The asset guarantor is a security role responsible for ensuring the development, use and security of the asset.

(4) The cybersecurity auditor

a) is a security role responsible for conducting cybersecurity audits; the exercise of this role may be entrusted to a person trained for this activity and demonstrating professional competence in conducting cybersecurity audits or audits of information security management systems

   1. for a period of at least three years, or

2. for a period of one year when graduated from university,

b) ensures that cybersecurity auditing is impartial, and
c) must not be entrusted with exercising other security roles.

(5) The obliged entity takes into account the recommendations given in Annex 6 hereto in determining the security role holders.

Section 8

Supplier management

(1) The obliged entity

a) establishes rules for suppliers that take into account the requirements of the information security management system,
b) keeps records of its important suppliers,
c) demonstrably notifies in writing its important suppliers of their records under letter b),
d) informs its suppliers of the rules referred to in a) and requires compliance with these rules,
e) manages the supplier-related risks,
f) in connection with the management of risks associated with important suppliers, ensures that contracts concluded with important suppliers include the relevant areas listed in Annex 7 hereto, and
g) regularly reviews the performance of contracts with important suppliers with respect to the information security management system.

(2) Furthermore in connection with important suppliers, the obliged entity

a) carries out, within the framework of the selection procedure and prior to conclusion of the contract, an assessment of the risks associated with the fulfilment of the selection procedure subject pursuant adequately to Annex 2 hereto,
b) establishes, within the framework of the contractual relations, the methods and levels of implementation of security measures and determine the content of the mutual contractual liability for the implementation and monitoring of security measures,
c) carries out a periodic risk assessment and periodic monitoring of the established security measures for performances provided by own resources or by a third party; and
d) provides solution in response to the risks and deficiencies identified.

(3) Requirements for demonstrably informing pursuant to paragraph 1, letter c) include

a) identification of operator or administrator,
b) identification of information and communication system,
c) identification of important supplier,

d) notification of the fact that the supplier is the important supplier for the operator and, where appropriate, also that the important supplier is also an administrator; and
e) content of the rules pursuant to paragraph 1, letter a).

(4) The obliged entity referred to in Section 3, letters c) to f) of the Act, which is an administrator and has been demonstrably notified pursuant to paragraph 1, letter c), reports the contact details in the form specified in Section 34.

Section 9

Security of human resources

(1) Within the framework of management of human resources security, the obliged entity

a) establishes, with regard to the state and needs of the information security management system, a security awareness development plan aimed at ensuring adequate education and security awareness raising, which includes the form, content and extent of
    1. instructing users, system administrators, security role holders and suppliers on their responsibilities and security policy, and
    2. necessary theoretical and practical training of users, system administrators and security role holders,
b) identifies the persons responsible for implementing individual activities envisaged in the plan,
c) instructs users, system administrators, security role holders and suppliers, in accordance with the security awareness development plan, on their responsibilities and the security policy through initial and regular trainings,
d) ensures regular professional training for those in charge of security roles in accordance with the security awareness development plan, taking into account the current needs of a cybersecurity obliged entity,
e) ensures regular training and verification of the staff safety awareness in line with the security awareness development plan, in accordance with their workload,
f) ensure that users, system administrators and security role holders are monitored for security policy compliance,
g) ensures the transfer of responsibilities in the event of termination of the contractual relationship with system administrators and security role holder,
h) evaluates the effectiveness of the security awareness development plan, conducted trainings and other security awareness raising activities, and
i) determines the rules and procedures for dealing with cases of breaches of security rules by users, system administrators and security role holders.

(2) The obliged entity keeps a summary of trainings pursuant to paragraph 1 that contains the subject of training and the list of persons who have completed the training.

Section 10

Operations and communications management

(1) Within the framework of operations and communications management, the obliged entity ensures the safe operation of the information and communication system and establishes rules and procedures which include, in particular

a) the rights and responsibilities of system administrators, users and security role holders,
b) procedures for starting and stopping the system, for restarting or restoring the system after failures and for treating fault states or extraordinary phenomena,
c) procedures for monitoring cybersecurity events and measures to protect access to records of such events,
d) rules and procedures for protection against malicious code,
e) managing technical vulnerabilities,
f) contacts for persons responsible for the performance of system and technical support,
g) procedures for the management and approval of operational changes,
h) procedures for monitoring, planning and managing the capacity of human and technical resources,
i) rules and procedures for the protection of information and data throughout the lifecycle,
j) rules and procedures for the installation of technical assets,
k) making regular backups and checking the usability of such backups made; and
l) rules and procedures to ensure the security of network services.

(2) Within the operations and communications management, the obliged entity complies with the rules and procedures laid down pursuant to paragraph 1 and updates these rules and procedures in relation to the changes made or planned.

(3) The obliged entity ensures the separation of the development, testing and operating environment.

Section 11

Change management

(1) Within the framework of management of changes in the information and communication system, the obliged entity

a) reviews the potential impacts of the changes, and
b) determines important changes.

(2) For important changes, the obliged entity

a) documents their management,
b) analyses risks,

c) takes measures to reduce any adverse effects associated with important changes,
d) updates the security policy and security documentation,
e) ensures their testing, and
f) ensures the possibility of returning to original state.

(3) The obliged entity referred to in Section 3, letters c), d) and f) of the Act on the basis of the results of the risk analysis pursuant to paragraph 2, letter b) decides to perform penetration testing or vulnerability testing; if the obliged entity decides to perform penetration testing or vulnerability testing, it proceeds in accordance with Section 25, paragraph 1 and responds to identified deficiencies.

(4) The obliged entity referred to in Section 3, letter e) of the Act is subject to the requirements in accordance with paragraph 3 in an appropriate manner.

Section 12

Access management

(1) The obliged entity, based on operational and security needs, manages the access to the information and communication system and takes measures to ensure the protection of data used to register under Sections 19 and 20 and to prevent the unauthorized use of such data.

(2) In managing the access to the information and communication system, the obliged entity further
a) manages access based on groups and roles,
b) assigns to each user and system administrator accessing the information and communication system access rights and permissions, and a unique identifier,
c) manages the identifiers, access rights and permissions of applications and technical accounts,
d) introduces security measures for managing the access of equipment to information and communication system resources,
e) introduces the security measures necessary for the safe use of mobile devices and other technical equipment, as well as the security measures related to the use of technical equipment which the obliged entity does not have in its administration,
f) limits the allocation of privileged permissions to the level strictly necessary for the workload performance,
g) limits and controls the use of program resources that may be able to overcome system or application controls,
h) assigns and withdraws access permissions in accordance with the access management policy,
i) performs a regular review of setting of all access permissions, including allocation to access groups and roles,
j) uses the identity management and verification tool as defined in Section 19 and the access permission management tool as defined in Section 20,

k) enforces the compliance of users with the established procedures when using private authentication information,
l) ensures the removal or change of access permissions when users, system administrators or security role holder change their position or change their inclusion,
m) ensures the removal or change of access permissions when contractual relationship is terminated or changed; and
n) documents allocation and removal of access permissions.

Section 13

Acquisitions, development and maintenance

The obliged entity, in connection with the planned acquisition, development and maintenance of the information and communication system

a) manages risks pursuant to Section 5,
b) manages important changes pursuant to Section 11,
c) determines the safety requirements,
d) includes safety requirements in the acquisition, development and maintenance projects,
e) ensures the security of the development and testing environment and ensure the protection of the test data used,
f) carries out security testing of important changes before they are put into service, and
g) fulfils the requirement under Section 19, paragraph 3, if it aims to the acquisition or development of the Identity Management and Verification Tool.

Section 14

Managing cybersecurity events and incidents

(1) In managing cybersecurity events and incidents, the obliged entity

a) introduces the process of detecting and evaluating cybersecurity events and managing cybersecurity incidents,
b) assigns responsibilities and establishes procedures for
    1. detecting and assessing cybersecurity events and incidents, and
    2. coordinating and managing cybersecurity incidents,
c) defines and applies procedures for identifying, collecting, retrieving and retaining credible evidence needed to analyse a cybersecurity incident,
d) ensures the detection of cybersecurity events,
e) in detection of cybersecurity events it further proceeds in accordance with Sections 22 and 23,
f) ensures that users, system administrators, security role holders, other staff and suppliers will report any unusual behaviour of the information and communication system and suspicion of any vulnerability,

g) ensure that cybersecurity events are assessed in order to decide whether they are to be classified as cybersecurity incidents in accordance with Section 31,
h) ensures that cybersecurity incidents are managed in accordance with established procedures,
i) takes measures to avert and mitigate the impact of cybersecurity incidents,
j) reports cybersecurity incidents in accordance with Section 32,
k) keeps track of cybersecurity incidents and how they are managed,
l) investigates and determines the causes of cybersecurity incidents, and
m) evaluates the effectiveness of the cybersecurity incident solution and, on the basis of the evaluation, decides on the necessary security measures or updates the existing security measures to avoid a repetition of the cybersecurity incident solved.

(2) In detecting cybersecurity events, the obliged entity referred to in Section 3, letters c), d) and f) of the Act uses the tool referred to in Section 24.

Section 15

Business continuity management

Within the framework of business continuity management, the obliged entity

a) establishes the rights and responsibilities of the system administrators and security role holders,
b) evaluates and documents the potential impacts of cybersecurity incidents through risk assessment and impact analysis and assesses possible risks associated with threats to the business continuity,
c) based on the outputs of the risk assessment and impact analysis under letter b), sets out the objectives of the business continuity management by determining
    1. the minimum level of services provided which is acceptable for the use, operation and management of the information and communication system,
    2. the recovery time during which, following a cybersecurity incident, the minimum level of services provided by the information and communication system is restored, and
    3. the data recovery point as the time period for which data after a cybersecurity incident or after failure has to be restored,
d) establishes a policy of the business continuity management that includes the fulfilment of the objectives under letter c),
e) develops, updates and regularly tests the business continuity plans and emergency plans related to the operation of the information and communication system and related services; and
f) implements measures to increase the resilience of the information and communication system to cybersecurity incidents and availability limitations, and in doing so it follows the requirements of Section 27.

Section 16

Cybersecurity audit

(1) Within the framework of cybersecurity audit, the obliged entity

a) carries out and documents a security policy compliance audit, including a review of technical compliance, and takes account of the audit results in the security awareness development plan and risk management plan; and
b) assesses the compliance of security measures with best practice, legislation, and internal regulations, other regulations and contractual obligations relating to the information and communication system, and determines possible corrective actions to ensure compliance.

(2) Audit pursuant to paragraph 1 is carried out

a) at important changes, within their scope,
b) at regular intervals of at least three years in the case of an obliged entity referred to in Section 3, letter e) of the Act, and
c) at regular intervals of at least two years in the case of an obliged person not referred to in point b).

(3) Where, in justified cases, it is not possible to carry out an audit at intervals pursuant to paragraph 2, letter b) and c) in its entirety, the audit may be carried out continuously, in systematic units. In such case, the entire audit must be completed within 5 years at the latest.

(4) The cybersecurity audit must be carried out by an entity meeting the conditions laid down in Section 7, paragraph 4, which independently assesses the correctness and effectiveness of the security measures in place.

(5) The obliged entity, which is at the same time the administrator, submits the results of the cybersecurity audit to the operator of the information and communication system.

TITLE II

TECHNICAL MEASURES

Section 17

Physical security

In terms of physical security, the obliged entity

a) prevents damage, theft or misuse of assets or the interruption of provision of the information and communication system services,
b) establishes a physical security perimeter that defines the area in which information is stored and processed and where technical assets of the information and communication system are located, and

c) for the physical security perimeter in accordance with letter b), introduces the necessary measures and applies the physical security means to
    1. prevent an unauthorized entry,
    2. prevent damage and unauthorized interventions, and
    3. provide protection at the level of premises and within the premises.

Section 18

Security of communication networks

To protect the security of the communications network included within the scope of Section 3, letter c), the obliged entity

a) ensures segmentation of the communication network,
b) ensures management of communication within the communication network and the communication network perimeter,
c) using cryptography, ensures the confidentiality and integrity of data upon remote access, remote management, or access to the communications network by means of wireless technologies,
d) actively blocks unwanted communications, and
e) uses a tool that ensures protection of the integrity of the communication network to ensure segmentation of the network and to manage the communication between its segments.

Section 19

Managing and authenticating identities

(1) The obliged entity uses a tool to manage and authenticate the identity of users, system administrators, and applications of the information and communication system.

(2) The tool for managing and authenticating users, system administrators, and applications ensures

a) verification of identity prior to commencement of activities in the information and communication system,
b) managing the number of possible unsuccessful login attempts,
c) resilience of stored or transmitted authentication data against unauthorized theft and misuse,
d) storing authentication data in a form resistant to off-line attacks,
e) re-authentication of the identity after a specified period of inactivity,
f) confidentiality of data authentication when access is restored, and
g) centralised identity management.

(3) The obliged entity uses an authentication mechanism to authenticate users, system administrators, and applications that is not based solely on the use of an account identifier and password, but rather on multifactor authentication with at least two different types of factors.

(4) Until the requirement in paragraph 3 is met, the tool for authentication of users, system administrators and applications must carry out authentication using cryptographic keys and guarantee a similar level of security.

(5) Until the requirements in paragraphs 3 or 4 are met, the tool for authentication of users, administrators and applications, which uses an account identifier and password to authenticate, must enforce following rules

a) the password length at least
   1. 12 characters for users and
   2. 17 characters for system administrators and applications,
b) allowing to enter a password of at least 64 characters,
c) the unrestricted use of lower and upper case letters, digits and special characters,
d) allowing users to change the password, with a period between two password changes not shorter than 30 minutes,
e) not allowing users and system administrators
   1. to choose most commonly used passwords,
   2. to create passwords based on multiple repeating characters, login name, e-mail, system name, or in a similar manner;
   3. to reuse previously used passwords with memory of at least 12 previous passwords, and
f) mandatory password change in an interval of maximally 18 months; this rule does not apply to accounts serving for system restoration in the event of a breakdown.

(6) Furthermore, the obliged entity in case of using authentication only by account and password

a) prompts change of the default password immediately after its first use,
b) immediately revokes a password for restoring access after its first use or expiry of not more than 60 minutes after its creation; and
c) compulsorily includes the rules for creating secure passwords in the security awareness development plan referred to in Section 9.

Section 20

Access permission management

The obliged entity uses a centralised tool for access authorization management to manage permissions

a) for access to individual assets of the information and communication system; and
b) for reading data, writing data and changing permissions.

Section 21

Protection against malicious code

(1) The obliged entity referred to in Section 3, letters c), d) and f) of the Act as part of the protection against malicious code

a) with regard to the importance of assets, ensures the use of the tool for continuous automatic protection of
   1. terminal stations,
   2. mobile devices,
   3. servers,
   4. data storages and removable data carriers,
   5. communication networks and communication network elements, and
   6. similar devices,
b) monitors and controls the use of removable devices and data carriers,
c) runs the automatic start-up of the contents of removable devices and data carriers,
d) manages permissions to run the code, and
e) performs a regular and effective update of the malicious code protection tool.

(2) The obliged entity referred to in Section 3, letter e) of the Act proceeds adequately in accordance with paragraph 1.

Section 22

Recording events of the information and communication system, its users and system administrators

(1) The obliged entity

a) records the security and necessary operational events of important assets of the information and communication system; and
b) based on the asset importance evaluation, updates the scope of assets for which security and operational events are recorded.

(2) The obliged entity ensures for recording of security and operational events pursuant to paragraph 1

a) a unique network identification of the originator's equipment when a tool is used in the communications network that changes its network identification,
b) gathering information on security and operational events; it particularly records
   1. the date and time including the time zone specification,
   2. type of activities,
   3. identification of the technical asset that recorded the activity,
   4. a unique identification of the account under which the activity was performed,

5. a unique network identification of the originator's equipment, and
6. success or failure of the activity,

c) the protection of information obtained under letters a) and b) from unauthorized reading and any alteration,

d) recording of
1. loging in/out for all accounts including failed attempts,
2. activities performed by administrators,
3. successful and unsuccessful handling of accounts, permissions, and rights,
4. failures to perform activities due to the lack of access rights and permissions,
5. user activities that may affect the security of the information and communication system,
6. starting and ending of activities of technical assets,
7. critical and error messages concerning technical assets; and
8. accesses to event logs, attempts to handle event logs, and changes to settings for event logging tools, and

e) synchronization of the uniform time of technical assets at least every 24 hours.

(3) The obliged entity referred to in Section 3, letters c), d) and f) of the Act retains records of the events recorded pursuant to paragraph 2 for at least 18 months.

(4) The obliged entity referred to in Section 3, letter e) of the Act retains records of the events recorded pursuant to paragraph 2 for at least 12 months.

Section 23

Detection of cybersecurity events

(1) The obliged entity within the communication network, which includes the information and communication system, uses a cybersecurity event detection tool to ensure

a) verification and control of the data transmitted within the communication network and between the communications networks,
b) verification and control of the data transmitted on the communication network perimeter, and
c) blocking of unwanted communications.

(2) The obliged entity referred to in Section 3, letter c), d) and f) of the Act ensures the detection of cybersecurity events proportionately to the importance of assets within the framework of

a) terminal stations,
b) mobile devices,
c) servers,
d) data storages and removable data carriers,
e) active network elements, and
f) similar assets.

Section 24

Collection and evaluation of cybersecurity events

The obliged entity referred to in Section 3, letters c), d) and f) of the Act uses a tool for collection and continuous evaluation of cybersecurity events that makes it possible to

a) collect and evaluate events recorded under Sections 22 and 23,
b) search for and group related records,
c) provide information for specified security roles about detected cybersecurity events,
d) evaluate cybersecurity events with the aim to identify cybersecurity incidents, including early warning of specified security roles,
e) limit instances of incorrect event evaluation by periodically updating the rules settings for
   1. evaluating cybersecurity events, and
   2. early warning, and
f) to use the information obtained by the tool for collection and evaluation of cybersecurity events for the optimal setting of security measures of the information and communication system.

Section 25

Application security

(1) The obliged entity carries out penetration tests of the information and communication system focusing on important assets, namely

a) before putting them into service, and
b) in connection with an important change pursuant to Section 11, paragraph 3.

(2) In addition, within the framework of application security, the obliged entity provides permanent protection of applications, information, and transactions against

a) unauthorized activity; and
b) denial of activities performed.

Section 26

Cryptographic means

To protect the assets of the information and communication system, the obliged entity

a) uses the current robust cryptographic algorithms and cryptographic keys,
b) uses the key and certificate management system, which
   1. ensures generation, distribution, storage, changes, validity limitation, invalidation of certificates and destruction of keys, and
   2. allows for control and audit,
c) promotes safe handling of cryptographic means, and
d) takes into account recommendation as for cryptographic means issued by the Agency, published on its website.

Section 27

Ensuring level of information availability

The obliged entity introduces measures ensuring the availability level to provide for

a) the availability of the information and communication system to meet the objectives set out in Section 15,
b) the resilience of the information and communication system to cybersecurity incidents that may reduce its availability,
c) the availability of important technical assets of the information and communication system, and
d) the redundancy of assets necessary to ensure the availability of the information and communication system.

Section 28

Industrial, control and similar specific systems

To ensure cybersecurity of industrial, control and similar specific systems, the obliged entity uses tools and measures to ensure

a) use of technical and program tools that are designed for a specific environment,
b) limitation of physical access to the equipment of these systems and to the communication network,
c) sorting out of the communication network intended for these systems from other infrastructure,
d) limitation and management of remote access to these systems,
e) protection of individual technical assets of these systems from the exploitation of known vulnerabilities, and
f) restoration of these systems after a cybersecurity incident.

Section 29

Digital services

(1) The obliged entity referred to in Section 3, letter h) of the Act introduces security measures pursuant to the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down detailed rules for application of Directive 2016/1148 of the European Parliament and of the Council as regards the specification of elements that the digital service providers have to take into account in the management the security risks faced by networks and information systems, and the parameters for assessing whether the impact of an incident is significant; the provisions of Sections 3 to 28 do not apply to that obliged person.

(2) The obliged entity referred to in Section 3, letter h) of the Act reports the contact details pursuant to Section 34, paragraph 2.

(3) The obliged entity referred to in Section 3, letter h) of the Act reports the cybersecurity incidents pursuant to Section 32, paragraphs 2 and 3.

TITLE III

SECURITY POLICY AND SECURITY DOCUMENTATION

Section 30

Security policy and security documentation

(1) The obliged entity

a) establishes a security policy and maintains security documentation covering the areas listed in Annex 5,
b) regularly reviews security policy and security documentation, and
c) keeps the security policy and security documentation up to date.

(2) Security policy and security documentation must be

a) available in paper or electronic form,
b) communicated within the obliged entity,
c) reasonably available to the parties concerned,
d) managed,
e) protected in terms of confidentiality, integrity and availability, and
f) maintained in such a way that the information contained therein is complete, legible, easily identifiable, and easilysearchable.

PART THREE

CYBERSECURITY INCIDENT

Section 31

Categorization of cybersecurity incidents

(1) Individual cybersecurity incidents are categorized by importance, taking into account

a) impacts contained in the impact determining criteria according to which the obliged entities were determined,
b) the number of affected users,
c) caused or expected damage,
d) importance of the assets concerned of the information and communication system,
e) impacts on the information and communication system services provided,
f) impacts on services provided by other information and communication systems,
g) the duration of the incident,
h) geographic scope of the area concerned, and
i) other impacts.

(2) For the purposes of cybersecurity incident reporting and handling, the cybersecurity incidents are classified into the following categories based on the account taken in paragraph 1

a) Category III – a very important cybersecurity incident that directly and importantly undermines the security of the provided services or assets. Its solution requires prompt intervention by the operator, with the need to prevent the further spread of the cybersecurity incident, including the minimization of both incurred and potential damages, by all available means,
b) Category II – an important cybersecurity incident that disrupts the security of the provided services or assets. Its solution requires prompt intervention by the operator, with the need to prevent the further spread of the cybersecurity incident, including the minimization of incurred damage, by appropriate means, or
c) Category I – a less important cybersecurity incident that causes a minor breach of security of the provided services or assets. Its solution requires intervention by the operator, with the need to limit the further spread of the cybersecurity incident, including the minimization of incurred damage, by appropriate means.

(3) Types of cybersecurity incidents by their impacts are as follows

a) a cybersecurity incident causing a breach of the confidentiality of assets,
b) a cybersecurity incident causing a breach of the integrity of assets,
c) a cybersecurity incident causing a breach of the availability of assets, or
d) a cybersecurity incident resulting in a combination of impacts referred to in letters a) to c).

(4) This provision does not apply to cybersecurity incidents at the obliged entity referred to in Section 3, letter h) of the Act.

Section 32

Form and requirements for reporting cybersecurity incidents

(1) The cybersecurity incident is reported to the Agency using an electronic form published on the Agency's website, sent

a) to the e-mail address of the Agency designated to receive cybersecurity incident reports, published on the Agency's website,
b) to the Agency 's data box, or
c) via data interface, if used, the description of which is published on the Agency's website.

(2) The cybersecurity incident is reported to the national CERT operator using an electronic form published on the website of the national CERT operator, sent

a) to the e-mail address of the national CERT operator designated to receive cybersecurity incident reports, published on their website,
b) to the data box of the national CERT operator, or
c) via the website of the national CERT operator.

(3) The cybersecurity incident report may also be sent in paper form, but only in cases where none of the methods mentioned in paragraphs 1 and 2 can be used.

(4) Requirements of the cybersecurity incident report are

a) the identification of the sender,
b) the identification of the information and communication system,
c) date and time of the incident detection, and
d) the incident description.

PART FOUR
REACTIVE MEASURES AND CONTACT DETAILS

Section 33
Reactive measures

(1) The obliged entity, which has been ordered by the Agency to execute a reactive measure,

a) evaluates the expected impacts of the reactive measure on the information and communication system and on the established security measures, and evaluates the possible negative effects; and
b) establishes a method for the rapid implementation of this measure, which minimizes its possible negative effects and specifies the timetable for its implementation.

(2) The obliged entity, which has been ordered by the Agency to execute a reactive measure, notifies the method for execution of the reactive measure and its result in the form provided on the Agency's website.

Section 34
Contact details

(1) The contact details are notified to the Agency using an electronic form published on the Agency's website, sent

a) to the e-mail address of the Agency designated to receive contact details, published on the Agency's website,
b) to the Agency’s data box, or
c) via data interface, if used, the description of which is published on the Agency's website.

(2) The contact details are notified to the national CERT operator using an electronic form published on the website of the national CERT operator, sent

a) to the e-mail address of the national CERT operator designated to receive contact details, published on their website,
b) to the data box of the national CERT operator, or
c) via the website of the national CERT operator.

(3) The contact details may also be sent in paper form, but only in cases where none of the methods referred to in paragraphs 1 and 2 can be used.

(4) The contact details notification form sample is shown in Annex 8 hereto.

(5) The obliged entity referred to in Section 3, letters c) to f) of the Act, which is the administrator, further attaches to the contact details notification pursuant to paragraph 1 a document, by which the operator demonstrably informs it pursuant to Section 8, paragraph 1, letter c).

PART FIVE
FINAL PROVISIONS

Section 35
Temporary provisions

(1) Within one year of the effective date of this Decree, the provisions of the Decree No. 316/2014 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures and on Establishing Reporting Requirements in the Area of Cybersecurity will apply to the content and structure of the security documentation and the content and scope of the established security measures in the case of critical information infrastructure information systems and critical information infrastructure communication systems that were determined prior to the effective date of this Decree, and in the case of important information systems that have met the relevant determining criteria prior to the effective date of this Decree.

(2) Within one year of the effective date of this Decree, this Decree will not apply to the method of disposal of data, operational data, information and copies thereof in the case of critical information infrastructure information systems and critical information infrastructure communication systems determined prior to the effective date of this Decree, and in the case of important information systems that have met the relevant determining criteria prior to the effective date of this Decree.

Section 36

Repealing clause

Decree No. 316/2014 Coll., on Security Measures, Cybersecurity Incidents, and Reactive Measures and on Establishing the Cybersecurity Reporting Requirements (the Cybersecurity Decree) is hereby repealed.

Section 37

Effectiveness

This Decree becomes effective on the day of its publication.

Director:

Ing. Navrátil m. p.

Annex 1 to the Decree No. 82/2018 Coll.

Asset Assessment

(1) For the assessment of the importance of assets, four-level rating scales are used in this case to evaluate the impact of information security breach on individual assets. The obliged entity may use a different number of levels for asset importance assessment than those set out in this Annex, provided that there is a clear link between the method for assessing the importance of assets used by it and the rating scales and levels of assessment identified in this Annex.

(2) It is recommended that every obliged person adapt these impact matrices to their needs.

Table 1: Confidentiality rating scale

Level	**Description**	**Examples of assets protection requirements**
Low	The assets are publicly accessible or intended for publication. A breach of the confidentiality of assets does not jeopardize the legitimate interests of the obliged entity. In the case of sharing such an asset with third parties and using the classification according to the Traffic Light Protocol (hereinafter referred to as the "TLP"), the TLP:WHITE designation is used.	No protection is required. Disposal/deletion of a Low-level asset - see Annex 4.
Medium	Assets are not publicly accessible and constitute the know-how of the obliged entity; the asset protection is not required by any legal regulation or contractual arrangement. In the case of sharing such an asset with third parties and using the classification according to TLP, especially TLP:GREEN or TLP:AMBER designations are used.	Access management means are used to protect confidentiality. Disposal/deletion of a Medium-level asset – see Annex 4.

High	Assets are not publicly accessible and their protection is required by law, other regulations or contractual arrangements (eg. business secrets, personal data). In the case of sharing such an asset with third parties and using the classification according to TLP, especially TLP:AMBER designation is used.	Access and record management means are used to protect confidentiality. Transmissions of information through the communications network are protected by cryptographic means. Disposal/deletion of a High-level asset – see Annex 4.
Critical	Assets are not publicly accessible and require above-standard protection beyond the previous category (eg. strategic business secrets, special categories of personal data). In the case of sharing such an asset with third parties and using the classification according to TLP, especially TLP:RED or TLP:AMBER designations are used.	Access and record management means are used to protect confidentiality as well as methods of protection against asset abuse by system administrators. Transmissions of information through the communications network are protected by cryptographic means. Disposal/deletion of a Critical-level asset – see Annex 4.

Table 2: Integrity rating scale

Level	**Description**	**Examples of assets protection requirements**
Low	The asset does not require any integrity protection. Disruption of the asset integrity does not jeopardize the legitimate interests of the obliged entity.	No protection is required.
Medium	The asset may require integrity protection. Disruption of the asset integrity may lead to the damage to the legitimate interests of the obliged entity and may have less severe impacts on primary assets.	For integrity protection, standard tools (eg. limiting the access rights for writing) are used.

High	The asset requires integrity protection. Disruption of the asset integrity leads to the damage to the legitimate interests of the obliged entity having significant impacts on primary assets.	Forintegrity protection, special tools are used to track the history of changes made and to record the identity of the person making the change. The protection of integrity of information transmitted by communications networks is secured by cryptographic means.
Critical	The asset requires integrity protection. Disruption of the asset integrity leads to very serious damage to the legitimate interests of the obliged entity having direct and very serious impacts on primary assets.	For integrity protection, special means of uniquely identifying the person making the change are used, (for example, using digital signature technology).

Table 3: Availability rating scale

Level	**Description**	**Examples of assets protection requirements**
Low	Disruption of availability of the asset is not important, and in the event of a failure, a longer period of time for remediation (up to 1 week) is normally tolerated.	Periodic backups are sufficient to protect availability.
Medium	Disruption of availability of the asset should not exceed one working day, any long-term failure leads to a potential threat to the legitimate interests of the obliged entity.	Common backup and recovery methods are used to protect availability.
High	Disruption of availability of the asset should not exceed several hours. Any failure must be dealt with promptly, as it directly threatens the legitimate interests of the obliged entity. Assets are considered very important.	Backup systems are used to protect availability and the service provision restoring may be conditioned upon the intervention by operator or technical asset exchange.
Critical	Disruption of availability of the asset is not permitted and even a short-term unavailability (lasting few minutes) leads to a serious threat to the legitimate interests of the obliged person. Assets are considered critical.	To protect availability, backup systems are used and service provision restoring is short-term and automated.

Risk assessment

(1) The unambiguous determination of the risk identification function is an essential part of the risk assessment methodology pursuant to Section 5.

(2) The risk value is most often expressed as a function influenced by the impact, threat and vulnerability.

(3) For example, the following function can be used for risk assessment:
Risk = impact × threat × vulnerability.

(4) In this case, the impact is derived from the asset assessment according to Annex 1.

(5) Where the obliged entity uses a risk assessment method that does not distinguish threat and vulnerability assessment, scales for threat and vulnerability assessment can be merged. Merging the scales should not lead to a loss of ability to distinguish the level of threat and vulnerability. For this purpose, a comment can be used that clearly outlines both the level of threat and the level of vulnerability. The same applies in cases where the obliged entity uses a different number of levels to evaluate impacts, threats, vulnerabilities and risks.

Table 1: Threat rating scale

Level	**Description**
Low	The threat does not exist or is less likely. The expected realization of the threat is not more than once in 5 years.
Medium	The threat is less likely to likely. The expected realization of the threat ranges from 1 to 5 years.
High	The threat is likely to very likely. The expected realization of the threat ranges from 1 month to 1 year.
Critical	The threat is very likely to more or less certain. The expected realization of the threat is more frequent than once a month.

Table 2: Vulnerability rating scale

Level	Description
Low	The vulnerability does not exist or vulnerability exploitation is unlikely. Security measures are in place that are able to detect vulnerabilities or any attempts to exploit them.
Medium	The vulnerability exploitation is less likely to likely. Security measures are in place and their effectiveness is regularly monitored. The capability of security measures to detect potential vulnerabilities or possible attempts to overcome measures in time is limited. No successful attempts to overcome security measures are known.
High	The vulnerability exploitation is likely to very likely. Security measures are in place, but their effectiveness does not cover all necessary aspects and is not regularly monitored. Partial successful attempts to overcome security measures are known.
Critical	The vulnerability exploitation is very likely to more or less certain. Security measures are not in place or their effectiveness is greatly limited. There is no control over the effectiveness of security measures. Successful attempts to overcome security measures are known.

Tab. 3: Risk rating scale

Level	Description
Low	The risk is considered acceptable.
Medium	The risk can be reduced by less demanding measures or, in case of more demanding measures, the risk is acceptable.
High	The risk is not acceptable in the long run and systematic steps must be taken to eliminate it.
Critical	The risk is inadmissible and steps must be taken without delay to eliminate it.

Annex 3 to the Decree No. 82/2018 Coll.

Vulnerabilities and threats

Warning: This annex contains only selected vulnerability and threat categories. Identifying specific vulnerabilities and threats is the responsibility of the obliged entity.

Vulnerabilities

1. Insufficient maintenance of the information and communication system
2. Obsolescence of the information and communication system
3. Insufficient protection of the outer perimeter
4. Insufficient security awareness of users and system administrators
5. Insufficient maintenance of the information and communication system
6. Inappropriate setting of access permissions
7. Insufficient procedures for identifying and detecting negative security phenomena, cybersecurity events and cybersecurity incidents
8. Insufficient monitoring of user and system administrator activity and inability to detect inappropriate or defective behaviour
9. Insufficient determination of security rules, imprecise or ambiguous definition of the rights and obligations of users, system administrators and security roles
10. Insufficient protection of assets
11. Inappropriate security architecture
12. Insufficient degree of independent control
13. Incapacity for early detection of errors by employees

Threats

1. Violation of security policy, unauthorized activity, misuse of permission by users and system administrators
2. Damage to or failure of hardware or software
3. Identity abuse
4. Use of software in violation of the license terms
5. Malicious code (eg. viruses, spyware, Trojan horses)
6. Physical security disruption
7. Interruption in the provision of electronic communications services or electricity supply
8. Misuse or unauthorized modification of data
9. Loss, theft or damage to the asset
10. Failure to comply with a contractual obligation on the part of the supplier
11. Employee error
12. Misuse of internal means, sabotage
13. Long-term interruption in the provision of electronic communications services, electricity supply or other important services

14. Lack of staff with the required professional level,
15. Targeted cyberattack using social engineering, use of spy techniques
16. Abuse of removable technical data carriers
17. Attack on electronic communication (interception, modification)

Annex 4 to the Decree No. 82/2018 Coll.

Data disposal

(1) This Annex sets out the obligations of the Information and Communication System Operator to define ways of deleting data and how to dispose of technical information carriers, operational data, information and copies thereof.

(2) Individual operators of the information and communication system establish rules for the deletion of data and disposal of technical data carriers in accordance with this Annex. This is without prejudice to the obligations under other legislation. It is necessary to choose an adequate level of service offering adequate security measures, including adequate rules for data deletion and disposal of technical data carriers, given the value and importance of assets.

(3) The rules on data disposal should be set proportionate to the value and importance of assets, and should take into account, in particular

a) value of the asset (particularly in terms of confidentiality),
b) technology (types and size of information carriers),
c) whether the information carrier is under the control of the organization or not,
d) whether the data is part of a dedicated or multi-tenant environment,
e) who will perform the disposal of data (internal employee or supplier),
f) availability of equipment and instruments for disposal,
g) capacity of the carriers being disposed of,
h) whether trained staff is available,
i) time requirements of the disposal,
j) cost of disposal with respect to the tools, training, validation, reuse of the information carrier
k) possible ways of data disposal (for example, destruction of the carrier, multiple overwriting of the data carrier, making data unreadable by encryption, and the like),
l) usable data disposal methods relative to the information carrier state (for example, in the case of damage to the device, it will not be possible to use the information overwrite option, but one of the methods of physical destruction).

(4) Methods of disposal of technical information carriers, operational data, information and copies thereof:

a) Removal
   1. The method of disposal consists of removing the data so that it is unavailable to the system (for example, removing the data file, throwing the printed document into the waste bin).
   2. It is the least secure way of data disposal. In the case of getting the information carrier, it is possible to recover the information with some effort.
   3. This method is not applicable to non-rewritable digital data carriers.
   4. Applicable method for the level of confidentiality of asset (based on Annex 1): low

b) Overwriting

1. The method of disposal consists of overwriting the protected information by random values. It is a medium-safe way of data disposal. Freely available tools do not allow the recovery of thus overwritten information.
2. Overwriting may be replaced or combined with safely disposal of cryptographic keys to encrypted information.
3. This method is not suitable for damaged media, non-rewritable media, or for high-capacity.
4. Applicable method for the level of confidentiality of asset (based on Annex 1): low to critical.

c) Physical destruction of information carrier

1. The method of disposal consists of destruction of the information carrier or disassembly of the device and subsequent destruction of the information carrier (by mechanical, chemical or thermal action).
2. It is the safest method of data disposal. The information carrier after physical destruction cannot be reused for the original purpose. Original information cannot be recovered even when spending a great deal of resources and efforts.
3. Applicable method for the level of confidentiality of asset (based on Annex 1): medium to critical.

Example of possible disposal methods according to the level of confidentiality of asset (based on Annex 1)

	Acceptable liquidation method according to the asset importance level			
Information carrier	**1. Low**	**2. Medium**	**3. High**	**4. Critical**
Information on a human-readable medium (printed documents, notes, and the like)	Removal: Throwing into the waste bin	Overwriting: Blackening. ---------- Physical destruction: Destruction of the information carrier using a shredder.	Physical destruction: Destroying the information carrier using a shredder with both longitudinal and cross cutting, by incineration or decomposition.	
Mobile devices (mobile phones, tablets)	Removal: Deleting information, resetting device to factory setting.	Overwriting: For devices with encrypted storage – removal of information and resetting to factory setting.	Physical destruction: Dismantling the equipment and destroying the information carrier.	
Network devices (router, switch, modem, and the like)	Removal: Deleting information,	Overwriting: Removal and clogging with artificial events		

<table>
<tr><td>Office equipment (scanner, printer, fax)</td><td>resetting device to factory setting.</td><td>(artificial network traffic, test print jobs, and the like)</td><td colspan="2"></td></tr>
<tr><td>Magnetic media (magnetic tapes, disks, HDD [Hard Disk Drive])</td><td rowspan="3">Removal:
Deleting data at the file system level.</td><td rowspan="3">Overwriting:
Data overwriting.
In the case of encrypted medium, an alternative is the safe disposal of cryptographic keys
----
Physical destruction.</td><td colspan="2"></td></tr>
<tr><td>Optical media (CD, DVD, HD-DVD, BLU-RAY)</td><td colspan="2" rowspan="2">Physical destruction:
Destroying the information carrier.</td></tr>
<tr><td>Electronic media (flash memory)</td></tr>
<tr><td>Outsourcing and cloud</td><td colspan="4">The acceptable way of disposing of data should be set out in a contractual arrangement.</td></tr>
<tr><td></td><td>Removal:
Removal of all files including previous versions.</td><td>Overwriting:
Using data storage encryption at the level of a storage medium and a safe disposal of cryptographic keys.

Alternatively, in the case of dedicated storage media, the data can be overwritten after termination of the service.</td><td>Overwriting:
Using data storage encryption at the level of a storage medium and a safe disposal of cryptographic keys stored in a customer-controlled certified Hardware Security Module (HSM) (for example, FIPS 140-2 Level 2 standard). Upon termination of the service, the top access key will be disposed of and data overwritten.</td><td>Overwriting/Physical destruction:
Use the method, see level “3. High” or use dedicated storage memory capacity. Upon termination of the service, the total sanitization of all used storage media should be performed according to the above mentioned rows for critical level.</td></tr>
</table>

Annex 5 to the Decree No. 82/2018 Coll.

Content of security policy and security documentation

1. Security policy

1.1. Information security management system policy

a) The objectives, principles and needs of the information security management
b) The scope and boundaries of the information security management system.
c) Rules and procedures for documentation management.
d) Rules and procedures for resource management and the operation of the information security management system.
e) Rules and procedures for conducting cybersecurity audits.
f) Rules and procedures for reviewing the information security management system.
g) Rules and procedures for corrective actions and improvement of information security management system.

1.2. Asset Management Policy

a) Identification, evaluation and registration of primary assets
    1. Determination and registration of individual primary assets, including determination of their guarantor,
    2. Assessment of the importance of primary assets in terms of confidentiality, integrity and availability.
b) Identification, evaluation and registration of supporting assets
    1. Determination and registration of individual supporting assets, including determination of their guarantor,
    2. Determination of links between primary and supporting assets.
c) Rules of protection for individual asset levels
    1. Ways of distinguishing between asset levels,
    2. Rules for asset manipulation and recording by asset level,
    3. Permissible uses of assets.
d) Methods for the reliable deletion or destruction of technical data carriers, information, operational data and copies thereof.

1.3. Organisational security policy

a) Determination of security roles and their rights and obligations.
b) Requirements for separation of the execution of activities of individual security roles.
c) Requirements for separation of the execution of security and operational roles.

1.4. Supplier management policy

a) Rules and principles for the selection of suppliers.
b) Rules for the assessment of risks related to suppliers.
c) Requirements of the service level agreement and the ways and levels of implementation of security measures and on the determination of mutual contractual liability.
d) Rules for the implementation of controls on the introduction of security measures.
e) Supplier rating rules.

1.5. Human resources security policy

a) Rules for the development of security awareness and methods for its evaluation
    1. Methods and forms for instructing users,
    2. Methods and forms for instructing asset guarantors,
    3. Methods and forms for instructing system administrators,
    4. Methods and forms for instructing security role holders.
b) Security training for new employees
c) Rules for dealing with violations of security policy of the information security management system.
d) Rules for termination of employment relationship or change of job position
    1. Return of the assets entrusted and the removal of rights upon termination of the employment relationship,
    2. Changing access permissions when changing the job position.

1.6 Operations and communications management policy

a) Competencies and responsibilities related to secure operation.
b) Procedures for secure operation.
c) Requirements and standards of secure operation.
d) Rules and limitations for conducting cybersecurity audits and security tests.

1.7. Access management policy

a) Principle of minimal permission / need to know.
b) Access management requirements.
c) Life cycle of access management.
d) Privileged permission management.
e) Emergency access management.
f) Regular review of access permissions including allocation of individual users in access groups.

1.8. Secure user behaviour policy

a) Rules for secure handling of assets.
b) Secure use of access password.
c) Secure use of electronic mail and Internet access.

d) Secure remote access.
e) Secure behaviour in social media.
f) Security in relation to mobile devices.

1.9. Policy of backup, recovery and long-term storage

a) Backup and recovery requirements.
b) Backup rules and procedures.
c) Long-term storage rules and procedures.
d) Rules for secure back-up and long-term information storage.
e) Recovery rules and procedures.
f) Backup and recovery testing rules and procedures.
g) Policy on access to backups, stored information.

1.10. Secure information handover and exchange policy

a) Rules and procedures for the protection of handed over information.
b) Methods of protecting the electronic exchange of information.
c) Rules for using cryptographic protection.

1.11. Technical vulnerability management policy

a) Rules for limiting the software installation.
b) Rules and procedures for searching for software repair packages.
c) Rules and procedures for testing software repairs.
d) Rules and procedures for deploying software repairs.

1.12. Secure use policy for mobile devices

a) Rules and procedures for secure use of mobile devices.
b) Rules and procedures for ensuring security of a device that the obliged entity does not have under its management.

1.13. Acquisition, development and maintenance policy

a) Security requirements for acquisition, development and maintenance.
b) Management of vulnerabilities.
c) Policy on the provision and acquisition of software licenses and information
    1. Rules and procedures for the deployment of software and its registration,
    2. Rules and procedures for checking compliance with the license terms.

1.14. Personal data protection policy

a) Characteristics of the processed personal data.
b) Description of adopted and implemented organizational measures for the personal data protection.

c) Description of adopted and implemented technical measures for the personal data protection.

1.15. Physical security policy

a) Object protection rules.
b) Rules for the control of entry of persons.
c) Device protection rules.
d) Detection of physical security breaches.

1.16. Communications Network Security Policy

a) Rules and procedures to ensure network security.
b) Determination of rights and obligations for secure operation of the network.
c) Rules and procedures for access control within the network.
d) Rules and procedures for protecting remote network access.
e) Rules and procedures for network monitoring and operational records evaluation.

1.17. Malicious code protection policy

a) Rules and procedures for network communication protection.
b) Rules and procedures for protecting servers and shared data storages.
c) Rules and procedures for the protection of workstations.

1.18. Policy for the deployment and use of a cybersecurity event detection tool

a) Rules and procedures for deploying a cybersecurity event detection tool.
b) Operating procedures for evaluating and responding to detected cybersecurity events.
c) Rules and procedures for optimizing the cybersecurity event detection tool setting.

1.19. Policy for the use and maintenance of a tool for collecting and evaluating cybersecurity events

a) Rules and procedures for recording and evaluating cybersecurity events.
b) Rules and procedures for the regular updating of rules for evaluating cybersecurity events.
c) Rules and procedures for the optimal setting of security features of the tool for collecting and evaluating cybersecurity events.

1.20. Safe use policy for cryptographic protection

a) Level of protection with respect to the type and strength of the cryptographic algorithm.
b) Rules for the cryptographic protection of information
    1. when transmitted over communications networks,
    2. when stored on a mobile device or a removable technical data carrier.
c) Key management system.

1.21. Change management policy

a) Method and principles of managing important changes within the obliged entity, their processes, information and communication systems.
b) Reviewing the impacts of important changes.
c) Method for recording and testing of important changes.

1.22. Policy to deal with cybersecurity incidents

a) Defining cybersecurity incident categories.
b) Rules and procedures for identifying, recording and managing individual categories of cybersecurity incidents.
c) Rules and procedures for testing the cybersecurity incident management system.
d) Rules and procedures for evaluating cybersecurity incidents and improving cybersecurity.
e) Keeping incident records.

1.23. Business continuity management policy

a) Rights and obligations of the persons involved.
b) Objectives of the business continuity management
    1. Minimum level of provided services,
    2. Restoration time, and
    3. Data restore point.
c) Business continuity management policy to meet the objectives of continuity.
d) Methods for evaluating the impact of cybersecurity incidents on continuity and the assessment of related risks.
e) Determination and content of the necessary continuity plans and emergency plans.
f) Procedures for the implementation of measures issued by the Agency.

2. Content of the security documentation

2.1. Cybersecurity audit report

a) Cybersecurity audit objectives.
b) Cybersecurity audit scope.
c) Cybersecurity audit criteria.
d) Identification of the team of auditors and persons involved in the cybersecurity audit.
e) Date and place where the cybersecurity audit activities were performed.
f) Cybersecurity audit findings.
g) Cybersecurity audit conclusions.

2.2. Report from the review of the information security management system

a) Evaluation of the measures from the previous review of the information security management system.

b) Identification of changes and circumstances that may affect the information security management system.
c) Feedback on the performance of the information security management
    1. Disagreements and corrective actions,
    2. Results of monitoring and measurement,
    3. Audit results,
    4. Fulfilment of the objectives of the information security management system.
d) Results of the risk assessment and the state of the risk management plan.
e) Identification of options for continuous improvement.
f) Recommendations for the necessary decisions, the determination of the measures and the persons performing the individual activities.

2.3. Methodology for identifying and evaluating assets and for risk assessment

a) Determining the rating scale for primary assets
    1. Determining the rating scale for the levels of asset confidentiality,
    2. Determining the rating scale for the levels of asset integrity,
    3. Determining the rating scale for the levels of asset availability.
b) Determining the rating scale for risks
    1. Determining the rating scale for impact levels,
    2. Determining the rating scale for threat levels,
    3. Determining the rating scale for vulnerability levels,
    4. Determining the rating scale for risk levels.
c) Methods and approaches to risk management.
d) Methods for approving acceptable risks.

2.4. Asset and risk assessment report

a) Overview of primary assets
    1. Identification and description of primary assets,
    2. Determination of primary asset guarantors,
    3. Assessment of primary assets in terms of confidentiality, integrity and availability.
b) Overview of supporting assets
    1. Identification and description of supporting assets,
    2. Determination of supporting asset guarantors,
    3. Determination of the links between primary and supporting assets.
c) Risk assessment
    1. Assessment of potential impacts on assets,
    2. Assessment of existing threats,
    3. Assessment of existing vulnerabilities, assessment of existing measures,
    4. Establishing the level of risk, comparing this level with the criteria for risk acceptability,
    5. Identification and approval of acceptable risks.
d) Risk management

1. Proposal for a method of risk management,
2. Proposal for measures and their implementation.

2.5. Declaration of applicability

a) Overview of the excluded security measures required by this Decree including the reasons why they were not applied.
b) Overview of security measures introduced, including the way they are implemented.

2.6. Risk management plan

a) Content and objectives of selected risk management measures including their links to specific risks.
b) Resources needed for individual risk management measures.
c) Persons arranging the individual security measures for risk management.
d) Deadlines for introducing individual security measures for risk management.
e) Method of implementing security measures.
f) Methods of rating the success of the implementation of individual security measures for risk management.

2.7. Security awareness development plan

a) Content and terms of instructing users, administrators, and security role holders.
b) Content and terms of instructing new employees.
c) Overviews containing each training topics and the list of persons who have completed the training.
d) Forms and methods of evaluating the plan.

2.8. Keeping change records

a) Records of life cycle of important changes.
b) Records of changes in the configuration of the supporting assets.

2.9. Notified contact details

Overview of notified contact details

2.10. Overview of generally binding legal regulations, internal regulations and other regulations and contractual obligations

a) Overview of generally binding legal regulations.
b) Overview of internal regulations and other regulations.
c) Overview of contractual obligations.

2.11. Other recommended documentation

a) Infrastructure topology.
b) Overview of network devices.

Annex No. 6 to the Decree 82/2018 Coll.

Committee on Cybersecurity Management and Security Roles

This Annex contains a description of recommended requirements for the Committee on Cybersecurity Management and the security roles mentioned in Sections 6 and 7.

Table 1: Committee on Cybersecurity Management

Role:	**Cybersecurity Management Committee**
Key activities	a) Responsibility for the overall management and development of cybersecurity within the framework of the obliged entity. b) Creation of a framework for cybersecurity, its course and principles for the obliged entity (defining strategic objectives and course of development in cybersecurity). c) Definition of roles and responsibilities within the information security management system. d) Definition of requirements for reporting and monitoring of the information security management system. e) Checking the current state of cybersecurity within the framework of the obliged entity and determining whether the planned objectives are being met.
Other conditions:	a) The member of the Cybersecurity Management Committee must be at least 1. a representative of top management or a person authorized by him/her, 2. a cybersecurity manager. b) The members of the Cybersecurity Management Committee meet regularly; the course and outcomes of the meetings are retained in paper or electronic form.

Table 2: Cybersecurity manager

Role:	**Cybersecurity Manager**
Key activities	a) Responsibility for managing the information security management system. b) Regular reporting for top management of the obliged entity. c) Regular communication with the top management of the obliged entity. d) Submission of the Asset and Risk Assessment reports, Risk Management plan, and Declaration of Applicability to the Cybersecurity Management Committee. e) Providing information security guidelines for creating, evaluating, selecting, managing and terminating ICT supplier relations. f) Communicating with GovCERT/CSIRT. g) Participating in the risk management process. h) Coordinating the incident management. i) Assessing the appropriateness and effectiveness of security measures.
Knowledge:	a) ISO/IEC 27000 and similar standards in the area of security and ICT. b) General knowledge of ICT (operating systems, databases, applications, data networks) with an emphasis on security c) Risk management. d) Business continuity management. e) Relevant legal and regulatory requirements, in particular the Act. f) Context of the obliged entity.
Experience:	a) Enforcement of the information security management system. b) Understanding risk definitions and risk scenarios. c) Risk management within the framework of the obliged entity. d) Ability to interpret the results of risk management and coordinate risk management.
Education and practice:	a) At least 3 years of practice in information or cyber security, or b) Graduation at the university level and at least one year of practice in information or cyber security.

Relevant certification*:	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Information Security Manager (accreditation scheme of the Czech Accreditation Institute - CAI).
Other conditions:	a) The role is incompatible with the roles responsible for the operation of information and communication systems and with other operational or managerial roles. b) For the proper performance of this role, the necessary powers, responsibilities and budget are needed.

Table 3: Cybersecurity architect

Role:	**Cybersecurity Architect**
Key activities	a) Responsibility for proposing the implementation of security measures. b) Ensuring the security architecture.
Knowledge:	a) Architecture of information and communication systems and its designing. b) Hardware components, tools and architecture. c) Operational systems and software. d) Business processes and their integration and ICT dependency. e) Security and risk management. f) Security of communications and networks. g) Identity and access management. h) Security assessment and testing. i) Security of operations. j) Basic principles of secure software development. k) Integration and dependency of ICT and business processes.
Experience:	a) Designing implementation of security measures. b) Designing security architecture with a focus on objectives and security. c) Software development security.
Education and practice:	a) At least 3 years of practice in information or cyber security, or b) Graduation at the university level and at least one year of practice in information or cyber security.

Relevant certification *:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Information Security Manageraccreditation scheme of the Czech Accreditation Institute - CAI).
Other conditions:	The role is incompatible with the roles responsible for the operation of information and communication systems.

Table 4: Cybersecurity auditor

Role:	**Cybersecurity Auditor**
Key activities	Conducting cybersecurity audits
Knowledge:	a) Methodology and frameworks of the information security audit. b) Internal audit processes and procedures. c) Internal audit roles and functions. d) Process of conducting the ICT security audit. e) Strategic and tactical ICT management. f) Acquisition, development and deployment of ICT. g) ICT operation, maintenance and service management. h) Protection of assets. i) Cybersecurity assessment, methods for testing and sampling. j) Relevant legislation. k) ICT security.
Experience:	a) Planning of information or cybersecurity audits. b) Conducting cybersecurity audits or information security management audits. c) Analysing audit results. d) Writing audit conclusions, presenting them and proposing recommendations to remedy the findings. e) Reporting of compliance with legal requirements. f) Conducting audits with a focus on ICT and information security or cybersecurity.
Education and practice:	a) At least 3 years of practice in information or cyber security audits, or b) Graduation at the university level and at least one year of practice in information or cyber security audits.

Relevant certification *:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management System (Lead Auditor ISMS), Auditor of information security (accreditation scheme of the Czech Accreditation Institute - CAI).
Other conditions:	a) The role is incompatible with the roles of 1. the Cybersecurity Management Committee, 2. the Cybersecurity Manager, 3. the Cybersecurity Architect, 4. the Asset Guarantor. b) The role is incompatible with the roles responsible for the operation of information and communication systems.

Table 5: Asset Guarantor

Role:	**Asset guarantor**
Key activities	a) Responsibility for ensuring the development, use and security of the asset. b) Collaboration with other security role holders.
Knowledge:	a) Good knowledge of the asset to which he/she is a guarantor. b) Good knowledge of internal security policies and methodologies (eg. the asset and risk assessment methodology).

*The certification may be other than that provided if the certification demonstrating the professional competence of the security role holders meets the requirements of ISO 17 024.

Annex 7 to the Decree No. 82/2018 Coll.

Supplier management – security measures for contractual relationships

The content of a contract concluded with important suppliers:

a) provisions of information security (in terms of confidentiality, availability and integrity),
b) provisions on the permission to use the data,
c) provisions on the authorship of the program code or, where applicable, of the program licenses,
d) provisions on supplier control and audit (customer audit rules),
e) provisions governing the chaining of suppliers, ensuring that the sub-suppliers undertake to fully comply with the arrangements between the obliged entity and the supplier and will not be in conflict with the requirements of the obliged entity on the supplier,
f) provisions on the supplier's obligation to comply with the security policy of the obliged entity or the provisions on the approval of the supplier's security policies by the obliged entity,
g) provisions on change management,
h) provisions on the compliance of contracts with generally binding legal regulations,
i) provisions on the obligation of the supplier to inform the obliged entity about
    1. the cybersecurity incidents related to contract performance,
    2. the method of risk management on the supplier's side and the residual risks associated with contract performance,
    3. any important change in the control of this supplier under the Commercial Corporation Act, or change in the ownership of the essential assets, or change in the right to dispose of these assets, used by that supplier for performance under the contract with the operator,
j) specification of the conditions in terms of security at the termination of the contract (eg. a transitional period when cooperation is terminated, but the service is still to be maintained before the deployment of a new solution, data migration, and the like),
k) specification of the conditions for the business continuity management in connection with the suppliers (eg. the inclusion of suppliers in emergency plans, suppliers' tasks in activating business continuity management),
l) specification of the conditions for the format of handing over the data, operational data and information, upon request by the operator,
m) data disposal rules,
n) provisions on the right to unilaterally withdraw from the contract in the event of an important change in control over the supplier or change in the control over the essential assets used by the supplier for performance under the contract, and
o) provisions on penalties for breach of obligations.

Annex 8 to the Decree No. 82/2018 Coll.

Sample Contact Details Notification Form

National Cyber Security Centre

Národní úřad pro kybernetickou a informační bezpečnost

ACS - Contact Details Notification Form			
Date:		Type of report:	*Initial reporting*
			Reporting changes
A: Details of the authority and person listed in Section 3 of the Act			
Name of the natural or legal person*:			
Type of authority and person*:	*CII/ESO/IIS Administrator*		
	Digital Service Provider		
	CII/ESO/IIS Operator		
Registered office address *:			
Identification number of the authority or person (ID) *:			
**** Attach to the form a copy of the document by which you have been informed by the System Operator that you are becoming an Administrator pursuant to Section 3 of Act No. 181/2014 Coll.**			
B: Identification of the information or communication system			
Name of the System Operator **:			
Name of the system*:			
Type of the system*:	*Critical information infrastructure (CII)*		
	Information system of essential service		
	Important information system (IIS)		
Information on the provided services and resources:			
Is the system available via the Internet?		*Yes*	*No*
Scope of public IP addresses:			
Domain names used:			

Type of the activity performed:**

☐	Management/operation	☐	Security surveillance
☐	Development	☐	Others
☐	System integrator		

C: Details on the natural person who is authorized by the authority or person referred to in Section 3 of the Act to act in matters governed by the Act

Name, Surname, incl. Title *:	Fixed phone line*:	Mobile phone line*:	E-mail*:	Role:

D: Important networks***

The entity providing the electronic communications network for CII:

NOTICE:

Current versions of the Contact Details Notification Form can be found on the Agency's website.

Please save the completed form as the PDF file and send it to the NÚKIB data box or send the form with a digital signature affixed to nckb@nukib.cz. DO NOT SEND SCANNED DOCUMENTS.

Delete as appropriate
* Required fields
** Applies only to the administrator
*** To be only filled by CII